Ex. A

BUSINESS | MEDIA

Efforts to Weed Out Fake Users for Online Advertisers Fall Short

Companies that claim to help brands avoid serving digital ads to bots regularly miss nonhuman traffic

By Patience Haggin Follow

Updated March 28, 2025 5:32 pm ET

ILLUSTRATION: EMIL LENDOF/WSJ, ISTOCK

Brands are spending billions of dollars on ads without knowing for sure that they are actually being shown to humans. The companies they pay to help figure that out are struggling with the task.

At least 40% of web traffic is made up of fake users, or computerized bots, according to cloud-services provider Cloudflare. And that share is expected to grow with the proliferation of artificial-intelligence systems that regularly scan the web for data to ingest.

A new report from Adalytics, a firm that helps brands analyze where their ads appear, says the top three companies that advertisers pay to detect and filter out bots—DoubleVerify, Integral Ad Science and Human Security—regularly miss nonhuman traffic. The report, shared exclusively with The Wall Street Journal, found tens of millions of instances over seven years in which ads for brands including Hershey's, Tyson Foods, T-Mobile, Diageo, the U.S. Postal Service and the Journal were served to bots across thousands of websites. This occurred even in cases when bots identified themselves as such, because they were used for benign purposes like archiving websites and detecting security threats.

The companies say they have comprehensive approaches to filtering out bots for clients. The advertisers declined to comment.

"It's like, can you tell the difference between a person and a person-shaped sock puppet that is holding up a sign saying, 'I am a sock puppet'?" said Laura Edelson, a computer science professor at Northeastern University and former Justice Department technologist who reviewed the Adalytics report at the Journal's request.

DoubleVerify previously called the Adalytics report "misleading and manufactured." The company said after this article was published that the Adalytics report and this story were "inaccurate and misleading" and that even when it doesn't catch bots before brands bid on ads, it often detects them after the fact and ensures advertisers don't pay for those ad impressions.

An Integral Ad Science spokeswoman said the company uses a combination of services both before and after brands bid on ads to help protect its customers. "We continuously evaluate and innovate our offerings to respond to today's rapidly changing digital landscape," she said. Human Security declined to comment on the Adalytics findings because it hadn't seen the full report.

Ad-verification vendors are paid to police auctions in which brands bid on banner ads and other website spots to get in front of potential shoppers. Advertisers pay the companies to make a split-second judgment on whether an ad will be shown to a human or a bot before locking in a purchase.

Adalytics doesn't work with companies on catching bots ahead of time but does compete with DoubleVerify, Integral Ad Science and Human Security on running analyses of bot exposure after the fact.

[redacted]

Blind Spots

The biggest giveaways that a web visitor might be a bot are found in the internet-protocol address and what programmers call the "user-agent"—credentials that appear when a website is visited, including the user's browser and device type, and whether the user announces itself as a bot.

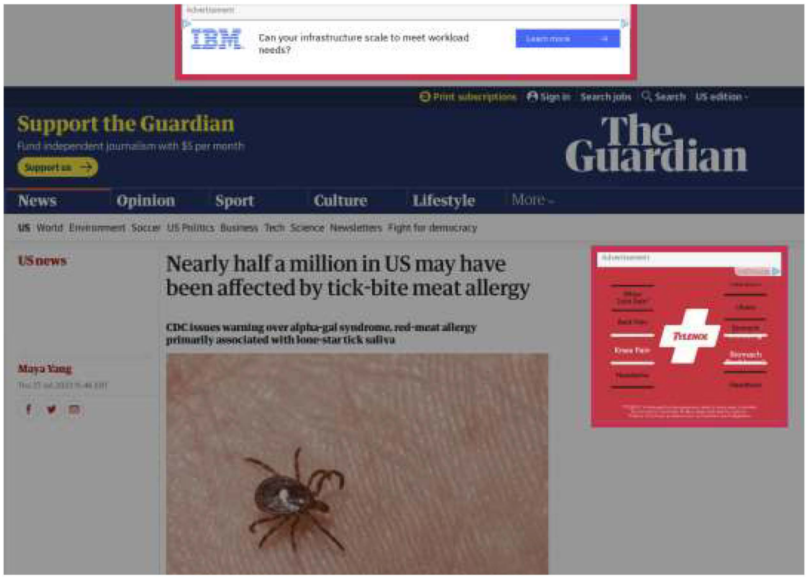
Yet some of the leading software that is supposed to help companies filter out bots before buying ads have major blind spots. Services from DoubleVerify and Integral Ad Science that try to catch bots before an advertiser bids don't receive those credentials from some of the largest ad-buying platforms, according to people familiar with the matter and a Wall Street Journal analysis of the platforms' applied programming interfaces for developers.

That means they don't always have the information needed to determine whether the user is a self-declared bot or if it is on industry-standard lists of known bots.

Integral Ad Science said in a blog post last Friday that even when it doesn't have access to certain credentials, it can provide advertisers with valuable information to avoid bidding on ad impressions for bots.

Executives at multiple ad agencies, publishers and brands told the Journal they were under the impression that DoubleVerify and Integral Ad Science could access the user-agent and IP addresses and relied on that information to filter out bots before bidding.

In one instance that Adalytics found, ads for International Business Machines and Tylenol appeared on a news story on the Guardian's website. The audience for the ads was a bot, not a human, even though multiple companies charged with filtering out bots were involved in the bid process.



Can your infrastructure scale to meet workload needs?

Nearly half a million in US may have been affected by tick-bite meat allergy

CDC issues warning over alpha-gal syndrome, red-meat allergy primarily associated with lone-star tick saliva

When a bot visited a news story on the Guardian's website, ads for IBM and Tylenol appeared. Multiple bot-filtration companies had vetted the user in the bid process yet none prevented the brands from bidding. PHOTO: URLSCAN

Kenvue, Tylenol's parent company, said it works with an outside ad verification vendor but didn't respond when asked to identify the company. IBM declined to comment. The Guardian said it takes steps to avoid having advertisements served to bots, and would make it up to brands if a significant portion of traffic for a campaign was misdirected.

Like the Guardian, The Wall Street Journal uses Integral Ad Science to help avoid ads being delivered to bots on its website. The Journal also uses DoubleVerify's product for publishers and has used DoubleVerify's product for advertisers via an ad agency.

One publisher that pays DoubleVerify to identify bots on its websites tested how well those efforts were going in November and came away disappointed. The publisher cross-referenced its reports from DoubleVerify with data on bot visits from security-scanning company URLScan.

DoubleVerify missed 21% of the documented bot visits and allowed ads to be served to them, according to the publisher's analysis and data reviewed by the Journal. In some cases, DoubleVerify's software identified a bot but still let a brand buy an ad for that audience, the analysis showed.

DoubleVerify declined to comment on the publisher's study.

Refund Status

Fighting fraud by bad actors—which don't flag themselves as bots—is even harder. Some scammers create bots to visit news sites, building up a browsing history that makes them look human to ad auctions. Then the bots visit websites the scammers own themselves, where advertisers bid on them because they look like promising shoppers. The scammers pocket the ad revenue.

Brands are supposed to be reimbursed if, after the fact, a verification company finds that a digital ad campaign had a significant audience of bots. Major ad-buying platforms that facilitate digital-ad auctions say they have refund processes for this situation. Yet ad buyers told the Journal they rarely seek refunds, since verification vendors report such low bot rates.

Quote.com, a comparison-shopping site for insurance products, spent hundreds of thousands of dollars on The Trade Desk's advertising services, including DoubleVerify's pre-bid filtering technology, in 2024. Erich Garcia, senior vice president of paid media, was given the full report by Adalytics and said the research made him question whether that was money well spent.

"It's as if you haven't even learned how to throw a baseball, but you want me to trust you to throw a hundred-mile-an-hour pitch," Garcia said.

Corrections & Amplifications
Quote.com, a comparison-shopping site for insurance products, spent hundreds of thousands of dollars on The Trade Desk's advertising services, including pre-bid filtering technology, in 2024. An earlier version of this article incorrectly said it spent hundreds of thousands of dollars on DoubleVerify's pre-bid filtering technology in 2024. (Corrected on March 29)

Write to Patience Haggin at patience.haggin@wsj.com